

VoIP güvenliği hakkında



ÇETİN KAYA
KOÇ

Geçtiğimiz on yıl içinde VoIP teknolojisi farklı mimariler üzerinde küresel ve ülkesel standart kuruluşları tarafından adreslendi.

Internet üzerinden akan veri trafiği, kendi binamızdan, yerel ağımızdan veya ülkemizden çıktuktan sonra artık bizim kontrolümüz altında değil. Dolayısıyla başkalarının kolaylıkla bu veriyi elde edip, içindeki bizim için önemli bilgilere ulaşması söz konusu. Veri için geçerli olan bu senaryo, VoIP yani Internet üzerinde ses trafiği içinde geçerli. Çünkü, ses bilgileri önce analogdan sayısala çevrilmekte, bu sayısal bilgiler sıkıştırılmakta, sonra RTP (real-time transport protocol) denilen bir metotla veri paketlerine dönüştürülmekte, ve en sonunda bu paketler, UDP datagramları içinde veri paketleri olarak ağda varış noktalarında doğru yönlendirilmektedir. Ağ trafiğinin bir kısmını eline geçiren bir kişi veya kurum UDP datagramlarından, RTP paketlerine ve oradan da analog konuşmaya ulaşıp, sizin konuşmanızı dinleyebilir.

Geçtiğimiz on yıl içinde VoIP teknolojisi farklı mimariler üzerinde küresel ve ülkesel standart kuruluşları tarafından adreslendi. Şimdi elimizde iki tane standart mimari var. Birincisi ITU (International Telecommunications Union) tarafından tanımlanmış olan H.323 isimli ses ve video için paket ağ çağrı ve sinyal sistemi. İkincisi ise SIP (session initiation protocol) denilen

ve IETF (internet engineering task force) tarafından geliştirilen iki yönlü haberleşme protokolü. SIP H.323e göre biraz daha basit bir protokol, ama aynı zamanda IETF'in tarihinde yayınladığı en uzun ve karmaşık bir protokol.

H.323 içinde güvenlik konularını adresleyen protokolün adı H.235. ITU standartları prensip olarak "özellik" zorlamadığı için ve güvenlikte bir "özellik" sayıldığı için, bu standard farklı güvenlik profilleri tanımlı yapılarak öneriler getiriyor. Bu öneriler de şirket, kurum ve ülkelerde uygulanarak, farklı çözümlere dönüşüyor. Birlikte çalışmayı (interoperability) sağlamak için bu profillerden birisi içinde olmak ve onu uygulamak lazım. H.235 gayet iyi ve detaylı tanımlanmış bir standart. SIP ise bir uygulama seviyesi (application-level) protokolü ve altyapıdaki transport protokolünden bağımsız. Ayrıca güvenlik için IETF'in zengin tecrübelerine ve var olan diğer güvenlik standartlarında (örneğin, S/MIME) dayanıyor. RFC 3261 standardı SIP güvenlik özelliklerini tanımlamak için yazılmış. SIP ve H.323 mimarileri birbirlerinden çok farklılar ve böylece güvenlik özellikleri de farklılıklar gösteriyor. Bunların üzerinde daha sonra konuşmaya devam edelim.

koc@krip.to